ABSTRACT OF THE DISCLOSURE

A method of identifying user, generating digital signature, and verifying digital signature by selecting a modulus p in the form of $p=(2^{dk}-2^{ck}-1)/r$; $p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r$; $p=(2^{dk}-2^{ck}-1)/r$; $p=(2^{dk}-2^{ck}+1)/r$; and $p=(2^{4k}-2^{3k}+2^{2k}+1)/r$; selecting an elliptic curve E and an order q; selecting a basepoint G; generating a private key w; generating a public key $W=wG$; distributing p, E, q, G, and W; retrieving a prover's private key w; retrieving the prover's public key W; generating a private integer k; combining k and the prover's G to form K using the prover's modulus p; sending K to the verifier; sending a challenge integer c to prover; combining c, k, and w to form a response integer v; sending v to the verifier; combining cG, K, and W using the prover's modulus p and checking to see if the combination is equal to vG. If not so, stop. Otherwise, retrieving the signer's private key w; generating a private integer k; combining k and G to form K using the prover's modulus p; combining K and a message M to form an integer h; combining h, k, and w to form an integer s; sending M and (K,s) as a digital signature of M; retrieving the prover's public key W; receiving M and (K,s); combining K and M to form an integer h; and combining h, k, and W using the prover's modulus p and checking to see if the combination is equal to sG. If so, the digital signature is verified.